CONSTRUCTION OF CLASS FIELDS OVER CYCLOTOMIC FIELDS

Ja Kyung Koo and Dong Sung Yoon

Abstract

Let ℓ and p be odd primes. For a positive integer μ let k_μ be the ray class field of $k = \mathbb{Q}(e^{\frac{2\pi i}{\ell}})$ modulo $2p^\mu$. We present certain class fields K_μ of k such that $k_\mu \le K_\mu \le k_{\mu+1}$, and find the degree of K_μ/k_μ explicitly. And by using Shimura's reciprocity law we also construct generators of the field K_μ over k_μ in terms of special values of theta constants.

1 Introduction

Let n be a positive integer, k be a CM-field with $[k : \mathbb{Q}] = 2n$, k^* be its reflex field and z_0 be the associated CM-point (§4). Shimura showed in [8] that if f is a Siegel modular function which is finite at z_0, then the special value $f(z_0)$ belongs to some abelian extension of k^*. And, his reciprocity law explains Galois actions on $f(z_0)$ in terms of action of the group $G_{\mathbb{A}+}$ on f (Proposition 4.2). Here $G_{\mathbb{A}+} = \prod'_p \mathrm{GSp}_{2n}(\mathbb{Q}_p) \times \mathrm{GSp}^+_{2n}(\mathbb{R})$ is the restricted product with respect to the subgroups $\mathrm{GSp}_{2n}(\mathbb{Z}_p)$ of $\mathrm{GSp}_{2n}(\mathbb{Q}_p)$. He also constructed in [7] Siegel modular functions by the quotient of two theta constants

$$\Phi_{(r,s)}(z) = \frac{\sum_{x\in\mathbb{Z}^n} e\left(\frac{1}{2}\,{}^t(x+r)z(x+r) + {}^t(x+r)s\right)}{\sum_{x\in\mathbb{Z}^n} e\left(\frac{1}{2}\,{}^txzx\right)}$$

for $r, s \in \mathbb{Q}^n$, and explicitly describe the Galois actions on the special values of theta functions (§3).

2010 *Mathematics Subject Classification.* 11G15, 11F46, 14H42.

Key words and phrases. cyclotomic fields, complex multiplication, Shimura's reciprocity law, Siegel modular forms, theta functions

This work was supported by the National Research Foundation of Korea grant funded by MEST (2011-0001184).

In this paper, we mainly consider the case where $k = \mathbb{Q}(e^{2\pi i/\ell})$ for an odd prime ℓ. Let p be an odd prime and μ be a positive ineteger. We denote by k_μ the ray class field of k modulo $2p^\mu$. Komatsu investigated in [4] a certain class field K_1 of k such that $k_1 \leq K_1 \leq k_2$ when $\ell = 5$, and constructed a normal basis of K_1 over k_1. In Section 5, we define the class field K_μ of k such that $k_\mu \leq K_\mu \leq k_{\mu+1}$, which generalizes the concept of K_1. We shall first find the exact degree of K_μ over k_μ for any odd prime ℓ (Theorem 5.5). And, we shall further provide a necessary and sufficient condition for K_μ to be the ray class field $k_{\mu+1}$ (Corollary 5.6). In Section 6, by making use of Shimura's reciprocity law we shall construct a basis of K_μ/k_μ in view of special values of $\Phi_{(r,s)}(z)$ for some $r, s \in \mathbb{Q}^n$ at the CM-point corresponding to the polarized abelian variety of genus $n = \frac{\ell-1}{2}$ (Theorem 6.3).

NOTATION 1.1. For $z \in \mathbb{C}$, we denote by $\overline{z}$ the complex conjugate of z and by $\mathrm{Im}(z)$ the imaginary part of z, and put $e(z) = e^{2\pi iz}$. If R is a ring with identity and $r, s \in \mathbb{N}$, $M_{r\times s}(R)$ indicates the ring of all $r \times s$ matrices with entries in R. In particular, we set $M_r(R) = M_{r\times r}(R)$. The identity matrix of $M_r(R)$ is written by 1_r and the transpose of a matrix α is denoted by ${}^t\alpha$. And, $R^\times$ stands for the group of all invertible elements of R. If G is a group and $g_1, g_2, \ldots, g_r$ are elements of G, let $\langle g_1, g_2, \ldots, g_r\rangle$ be the subgroup of G generated by $g_1, g_2, \ldots, g_r$, and G^n be the subgroup $\{g^n \mid g \in G\}$ of G for $n \in \mathbb{N}$. Moreover, if H is a subgroup of G, let $|G : H|$ be the index of H in G. For a finite algebraic extension K over F, $[K : F]$ denotes the degree of K over F. We let $\zeta_N = e^{2\pi i/N}$ be a primitive Nth root of unity for a positive integer N.

2 Siegel modular forms

We shall briefly introduce necessary facts about Siegel modular forms and explain action of $G_{\mathbb{A}+}$ on the Siegel modular functions whose Fourier coefficients are in some cyclotomic fields.

Let n be a positive integer and G be the algebraic subgroup of GL_{2n} defined over $\mathbb{Q}$ such that

$$G_{\mathbb{Q}} = \left\{\alpha \in GL_{2n}(\mathbb{Q}) \mid {}^t\alpha J\alpha = \nu(\alpha)J \ \text{ with } \nu(\alpha) \in \mathbb{Q}^\times\right\},$$

where

$$J = J_n = \begin{pmatrix} 0 & -1_n \\ 1_n & 0 \end{pmatrix}.$$

Considering ν as a homomorphism $G_{\mathbb{Q}} \to \mathbb{Q}^\times$ we denote its kernel by $Sp_{2n}(\mathbb{Q})$, namely

$$Sp_{2n}(\mathbb{Q}) = \{\alpha \in G_{\mathbb{Q}} \mid {}^t\alpha J\alpha = J\},$$

and let $Sp_{2n}(\mathbb{Z}) = Sp_{2n}(\mathbb{Q}) \cap GL_{2n}(\mathbb{Z})$. We set $G_{\mathbb{Q}+} = \{\alpha \in G_{\mathbb{Q}} \mid \nu(\alpha) > 0\}$ and let $\mathbb{H}_n = \{z \in M_n(\mathbb{C}) \mid {}^t z = z,\ \mathrm{Im}(z) > 0\}$ be the Siegel upper half-space of degree n. Here, for a hermitian matrix ξ we write $\xi > 0$ to mean that ξ is positive definite.

Now, define the action of an element $\alpha = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ of $G_{\mathbb{Q}+}$ on $\mathbb{H}_n$ by

$$\alpha(z) = (Az + B)(Cz + D)^{-1},$$

where $A, B, C, D \in M_n(\mathbb{Q})$. For every positive integer N, let

$$\Gamma(N) = \big\{\gamma \in Sp_{2n}(\mathbb{Z}) \mid \gamma \equiv 1_{2n} \pmod{N \cdot M_{2n}(\mathbb{Z})}\big\}.$$

A symmetric matrix $\xi \in GL_n(\mathbb{Q})$ is called *half-integral* if 2ξ is an integral matrix whose diagonal entries are even. For an integer m, a holomorphic function $f : \mathbb{H}_n \to \mathbb{C}$ is called a *(classical) Siegel modular form of weight m and level N* if

$$f(\gamma(z)) = \det(Cz + D)^m f(z) \tag{2.1}$$

for all $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma(N)$ and $z \in \mathbb{H}_n$, plus for $n = 1$ the requirement that f is holomorphic at every cusp. In particular, $f(z)$ has a Fourier expansion of the form

$$f(z) = \sum_{\xi\ half-integral} A(\xi) e(tr(\xi z)/N)$$

with $A(\xi) \in \mathbb{C}$, where ξ runs over all positive semi-definite half-integral matrices of degree n [3, §4 Theorem 1].

For a subring R of $\mathbb{C}$, let $\mathfrak{M}_m\big(\Gamma(N), R\big)$ be the vector space of all Siegel modular forms f of weight m and level N whose Fourier coefficients $A(\xi)$ belong to R and let $\mathfrak{M}_m(R) = \bigcup_{N=1}^{\infty} \mathfrak{M}_m\big(\Gamma(N), R\big)$. We denote by $\mathfrak{A}_m(R)$ the set of all meromorphic functions of the form g/h with $g \in \mathfrak{M}_{r+m}(R),\ 0 \neq h \in \mathfrak{M}_r(R)$ (with any $r \in \mathbb{Z}$), and by $\mathfrak{A}_m\big(\Gamma(N), R\big)$ the set of all $f \in \mathfrak{A}_m(R)$ satisfying (2.1).

Now, let $G_{\mathbb{A}}$ be the adelization of G, G_0 the non-archimedean part of $G_{\mathbb{A}}$, and G_∞ the archimedean part of $G_{\mathbb{A}}$. We extend the multiplier map $\nu : G_{\mathbb{Q}} \to \mathbb{Q}^\times$ to a continuous map of $G_{\mathbb{A}}$ into $\mathbb{Q}_{\mathbb{A}}^\times$, which we denote again by ν. Then we put $G_{\infty+} = \{x \in G_\infty \mid \nu(x) \gg 0\}$ and $G_{\mathbb{A}+} = G_0 G_{\infty+}$. Here $t \gg 0$ means $t_v > 0$ for all archimedean primes v of $\mathbb{Q}$. For every algebraic number field F, let F_{ab} be the maximal abelian extension of F, and $F_{\mathbb{A}}^\times$ the idele group of F. By class field theory, every element x of $F_{\mathbb{A}}^\times$ acts on F_{ab} as an automorphism. We then denote this automorphism by $[x, F]$. On the other hand, every element of $G_{\mathbb{A}+}$ acts on $\mathfrak{A}_0(\mathbb{Q}_{ab})$ as an automorphism ([7, p.680]). If $x \in G_{\mathbb{A}+}$ and $f \in \mathfrak{A}_0(\mathbb{Q}_{ab})$, we denote by f^x the image of f under x.

For a positive integer N, let

$$\begin{aligned} R_N &= \mathbb{Q}^\times \cdot \{a \in G_{\mathbb{A}+} \mid a_q \in GL_{2n}(\mathbb{Z}_q), a_q \equiv 1_{2n} \pmod{N \cdot M_{2n}(\mathbb{Z}_q)} \text{ for all rational primes } q\}, \\ \triangle &= \left\{ \begin{pmatrix} 1_n & 0 \\ 0 & x \cdot 1_n \end{pmatrix} \mid x \in \prod_q \mathbb{Z}_q^\times \right\}. \end{aligned}$$

PROPOSITION 2.1. *For every positive integer N, we have*

$$G_{\mathbb{A}+} = R_N \triangle G_{\mathbb{Q}+}.$$

PROOF. [9, Proposition 3.4] and [10, p.535 (3.10.3)]. □

PROPOSITION 2.2. *Let $f(z) = \sum_\xi A(\xi) e(tr(\xi z)/N) \in \mathfrak{A}_0\big(\Gamma(N), \mathbb{Q}(\zeta_N)\big)$. Then we get the followings:*

(i) *$f^\beta = f$ for $\beta \in R_N$. Moreover, $\mathfrak{A}_0\big(\Gamma(N), \mathbb{Q}(\zeta_N)\big)$ is the subfield of $\mathfrak{A}_0(\mathbb{Q}_{ab})$ consisting of all the R_N-invariant elements.*

(ii) *Let $y = \begin{pmatrix} 1_n & 0 \\ 0 & x \cdot 1_n \end{pmatrix} \in \triangle$ and t be a positive integer such that $t \equiv x_q \pmod{N\mathbb{Z}_q}$ for all rational primes q. Then we derive*

$$f^y = \sum_\xi A(\xi)^\sigma e(tr(\xi z)/N),$$

where σ is the automorphism of $\mathbb{Q}(\zeta_N)$ such that $\zeta_N^\sigma = \zeta_N^t$.

(iii) *$f^\alpha = f \circ \alpha$ for $\alpha \in G_{\mathbb{Q}+}$.*

PROOF. [7, p.681] and [8, Theorem 26.8]. □

3 Theta functions

In this section we shall provide necessary fundamental transformation formulas of theta functions and describe action of $G_{\mathbb{A}+}$ on the quotient of two theta-constants.

Let n be a positive integer, $u \in \mathbb{C}^n$, $z \in \mathbb{H}_n$ and $r, s \in \mathbb{R}^n$. We define a (classical) *theta function* by

$$\Theta(u, z; r, s) = \sum_{x \in \mathbb{Z}^n} e\Big(\frac{1}{2} \cdot {}^t(x+r) z (x+r) + {}^t(x+r)(u+s)\Big).$$

PROPOSITION 3.1. *Let $r, s \in \mathbb{R}^n$ and $a, b \in \mathbb{Z}^n$.*

(i) $\Theta(-u, z; -r, -s) = \Theta(u, z; r, s)$.

(ii) $\Theta(u,z;r+a,s+b)=e({}^trb)\Theta(u,z;r,s)$.

PROOF. [7, p.676 (13)]. □

For a square matrix S, by $\{S\}$ we mean the column vector whose components are the diagonal elements of S.

PROPOSITION 3.2. *For every* $\gamma=\begin{pmatrix}A & B\\ C & D\end{pmatrix}\in\Gamma(1)$ *such that* $\{{}^tAC\},\{{}^tBD\}\in 2\mathbb{Z}^n$, *we get the transformation formula*

$$\Theta\big({}^t(Cz+D)^{-1}u,\gamma(z);r,s\big)=\lambda_\gamma e\Big(\frac{{}^trs-{}^tr's'}{2}\Big)\det(Cz+D)^{1/2}e\big(\frac{1}{2}\cdot{}^tu(Cz+D)^{-1}cu\big)\Theta(u,z;r',s'),$$

where λ_γ *is a constant of absolute value 1 depending only on* γ *and the choice of the branch of* $\det(Cz+D)^{1/2}$, *and*

$$\begin{pmatrix}r'\\ s'\end{pmatrix}={}^t\gamma\begin{pmatrix}r\\ s\end{pmatrix}.$$

In particular, $\lambda_\gamma^4=1$ *for* $\gamma\in\Gamma(2)$.

PROOF. [7, Proposition 1.3 and Proposition 1.4]. □

Here, the functions $\Theta(0,z;r,s)$ are called *theta-constants*, and these are holomorphic on $\mathbb{H}_n$ as functions in z ([7, Proposition 1.6]).

PROPOSITION 3.3. *Suppose that* r,s *belong to in* $\mathbb{Q}^n$. *Then the theta constant* $\Theta(0,z;r,s)$ *represents the zero function if and only if* $r,s\in\frac{1}{2}\mathbb{Z}^n$ *and* $e(2\cdot{}^trs)=-1$.

PROOF. [2, Theorem 2]. □

Let

$$\Phi_{(r,s)}(z)=\frac{\Theta(0,z;r,s)}{\Theta(0,z;0,0)}.$$

Note that the poles of $\Phi_{(r,s)}(z)$ are exactly the zeros of $\Theta(0,z;0,0)=\sum_{x\in\mathbb{Z}^n}e\Big(\frac{1}{2}\ {}^txzx\Big)$. When $n=1$, $\Theta(0,z;0,0)$ has no zero on $\mathbb{H}_1$ by Jacobi's triple product identity [1, Theorem 14.6].

LEMMA 3.4. *For* $r,s\in\mathbb{R}^n$ *and* $a,b\in\mathbb{Z}^n$, *we achieve that*

(i) $\Phi_{(-r,-s)}(z)=\Phi_{(r,s)}(z)$,

(ii) $\Phi_{(r+a,s+b)}(z)=e({}^trb)\Phi_{(r,s)}(z)$,

(iii) *If* $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma(1)$ *such that* $\{{}^tAC\}, \{{}^tBD\} \in 2\mathbb{Z}^n$, *then we obtain*

$$\Phi_{(r,s)}\big(\gamma(z)\big) = e\Big(\frac{{}^trs - {}^tr's'}{2}\Big)\Phi_{(r',s')}(z),$$

where

$$\begin{pmatrix} r' \\ s' \end{pmatrix} = {}^t\gamma \begin{pmatrix} r \\ s \end{pmatrix}.$$

Proof. It is immediate from Proposition 3.1 and Proposition 3.2. □

Proposition 3.5. *Let* μ *and* m *be positive integers and let* $r, s \in \frac{1}{m}\mathbb{Z}^n$. *Then* $\Phi_{(r,s)}(\mu z)$ *belongs to* $\mathfrak{A}_0\big(\Gamma(2\mu m^2), \mathbb{Q}_{ab}\big)$. *Moreover, if* x *is an element of* $\triangle$ *such that*

$$x_q \equiv \begin{pmatrix} 1_n & 0 \\ 0 & t1_n \end{pmatrix} \mod 2\mu m^2 M_{2n}(\mathbb{Z}_q)$$

for all rational primes q *and a positive integer* t, *then*

$$\Phi_{(r,s)}(\mu z)^x = \Phi_{(r,ts)}(\mu z).$$

Proof. [7, Proposition 1.7]. □

Corollary 3.6. *For* $m \in \mathbb{N}$ *and* $r, s \in \frac{1}{m}\mathbb{Z}^n$, *let*

$$y = \beta \begin{pmatrix} 1_n & 0 \\ 0 & x \cdot 1_n \end{pmatrix} \alpha \in G_{\mathbb{A}+}$$

with $\beta \in R_{2m^2}$, $x \in \prod_q \mathbb{Z}_q^\times$, *and* $\alpha \in G_{\mathbb{Q}+}$. *Then*

$$(\Phi_{(r,s)})^y(z) = \Phi_{(r,ts)}\big(\alpha(z)\big),$$

where t *is a positive integer such that* $t \equiv x_q \pmod{2m^2\mathbb{Z}_q}$ *for all rational primes* q.

Proof. This can be proved by Proposition 2.2 and Proposition 3.5. □

4 Shimura's reciprocity law

We begin with fundamental but necessary facts about Shimura's reciprocity law [8, §26].

Let n be a positive integer, K be a CM-field with $[K : \mathbb{Q}] = 2n$ and $\mathcal{O}_K$ be a ring of integers of K. And, let $\varphi_1, \varphi_2, \ldots, \varphi_n$ be n distinct embeddings of K into $\mathbb{C}$ such that there are no two embeddings among them which are complex conjugate of each other on K. Then $(K; \{\varphi_1, \varphi_2, \ldots, \varphi_n\})$ is a CM-type and we can take an element ρ in K such that

(i) ρ is purely imaginary,

(ii) $-\rho^2$ is totally positive,

(iii) $\mathrm{Im}(\rho^{\varphi_i}) > 0$ for all $i = 1, \ldots, n$,

(iv) $\mathrm{Tr}_{K/\mathbb{Q}}(\rho x) \in \mathbb{Z}$ for all $x \in \mathcal{O}_K$.

We denote by $v(\beta)$, for $\beta \in K$, the vector of $\mathbb{C}^n$ whose components are $\beta^{\varphi_1}, \ldots, \beta^{\varphi_n}$. Let $L = \{v(\alpha) \mid \alpha \in \mathcal{O}_K\}$ be a lattice in $\mathbb{C}^n$. For $z = {}^t(z_1, z_2, \ldots, z_n)$ and $w = {}^t(w_1, w_2, \ldots, w_n)$ in $\mathbb{C}^n$, we define an $\mathbb{R}$-bilinear form $E(z, w)$ on $\mathbb{C}^n$ by

$$E(z, w) = \sum_{i=1}^{n} \rho^{\varphi_i}(z_i \overline{w_i} - \overline{z_i} w_i).$$

Then E becomes a non-degenerate Riemann form on the complex torus $\mathbb{C}^n/L$ satisfying

$$E\big(v(\alpha), v(\beta)\big) = \mathrm{Tr}_{k/\mathbb{Q}}(\rho\alpha\overline{\beta}) \quad \text{for } \alpha, \beta \in K,$$

which makes it a polarized abelian variety ([8, p.43–44]). Hence we can find a positive integer δ, a diagonal matrix ϵ with integral elements, and a complex $(n \times 2n)$-matrix Ω such that

(i) $E(\Omega x, \Omega y) = \delta \cdot {}^t x J y \quad \text{for } (x, y) \in \mathbb{R}^{2n} \times \mathbb{R}^{2n}$,

(ii) $L = \left\{ \Omega \begin{pmatrix} a \\ b \end{pmatrix} \;\middle|\; a \in \mathbb{Z}^n, b \in \epsilon\mathbb{Z}^n \right\}$,

(iii) $\epsilon = \begin{pmatrix} \epsilon_1 & & & \\ & \epsilon_2 & & \\ & & \ddots & \\ & & & \epsilon_n \end{pmatrix}$, $\epsilon_1 = 1$, $\epsilon_i \mid \epsilon_{i+1} \quad \text{for } i = 1, \ldots, n-1$.

([8, Lemma 27.2] or [7, p.675]). Now, we write $\Omega = (\Omega_1 \;\; \Omega_2) = \big(v(e_1) \;\; v(e_2) \;\; \cdots \;\; v(e_{2n})\big)$ with $\Omega_1, \Omega_2 \in M_n(\mathbb{C})$ and $e_1, e_2, \ldots, e_{2n} \in K$, and put $z_0 = \Omega_2^{-1}\Omega_1$. It is well-known that $z_0 \in \mathbb{H}_n$. Let $\Phi : K \to M_n(\mathbb{C})$ be a ring monomorphism such that

$$\Phi(\alpha) = \begin{pmatrix} \alpha^{\varphi_1} & & & \\ & \alpha^{\varphi_2} & & \\ & & \ddots & \\ & & & \alpha^{\varphi_n} \end{pmatrix} \quad \text{for } \alpha \in K.$$

Then we can define a ring monomorphism $h : K \to M_{2n}(\mathbb{Q})$ by

$$\Phi(\alpha)\Omega = \Omega \cdot {}^t h(\alpha) \quad \text{for } \alpha \in K.$$

Here, $h(\alpha) = \big(a_{ij}\big)_{1\le i,j\le 2n}$ is in fact the regular representation of α with respect to $\{e_1, e_2, \dots, e_{2n}\}$, namely $\alpha e_i = \sum_{j=1}^{2n} a_{ij} e_j$. If $\epsilon = 1_n$, then $L = v(\mathcal{O}_K) = \Omega \cdot \mathbb{Z}^{2n} = \mathbb{Z}v(e_1) + \cdots + \mathbb{Z}v(e_{2n})$ so that $h(\omega) \in M_{2n}(\mathbb{Z})$ for $\omega \in \mathcal{O}_K$. One can then readily show that

$$h(\overline{\alpha}) = J\, {}^t h(\alpha) J^{-1} \quad \text{for } \alpha \in K,$$

and z_0 is the CM-point of $\mathbb{H}_n$ induced from h which corresponds to the principally polarized abelian variety $(\mathbb{C}^n/L, E)$ ([7, p.684-685] or [8, §24.10]). In particular, if we put $S = \{\alpha \in K^\times \mid \alpha\overline{\alpha} \in \mathbb{Q}^\times\}$ then $h(S) = \{\alpha \in G_{\mathbb{Q}+} \mid \alpha(z_0) = z_0\}$.

Let K^* be the reflex field of K and K' be a Galois extension of K over $\mathbb{Q}$, and extend φ_i $(i = 1, \dots, n)$ to an element of $\mathrm{Gal}(K'/\mathbb{Q})$, which we denote again by φ_i. Let $\{\psi_j\}_{j=1}^m$ be the set of all the embeddings of K^* into $\mathbb{C}$ obtained from $\{\varphi_i^{-1}\}_{i=1}^n$.

Proposition 4.1. *Let K, K^* and $\{\psi_j\}$ be as above.*

(i) *$(K^*; \{\psi_1, \dots, \psi_m\})$ is a primitive CM-type and we have*

$$K^* = \mathbb{Q}\Big(\sum_i \alpha^{\varphi_i} \mid \alpha \in K\Big).$$

(ii) *If $\beta = \prod_j \alpha^{\psi_j}$ with $\alpha \in K^*$, then $\beta \in K$ and $\beta\overline{\beta} = N_{K^*/\mathbb{Q}}(\alpha)$.*

Proof. [8, p.62–63]. □

We call the CM-type $(K^*; \{\psi_j\})$ the *reflex* of $(K; \{\varphi_i\})$. By Proposition 4.1, we can define a homomorphism $\varphi^* : (K^*)^\times \to K^\times$ by

$$\varphi^*(a) = \prod_{j=1}^m a^{\psi_j} \quad \text{for } a \in (K^*)^\times,$$

and we have $\varphi^*(a) \cdot \overline{\varphi^*(a)} = N_{K^*/\mathbb{Q}}(a)$ for $a \in (K^*)^\times$. The map h can be extended naturally to a homomorphism $K_{\mathbb{A}} \to M_{2n}(\mathbb{Q}_{\mathbb{A}})$, which we also denote by h. Then for every $b \in (K^*)_{\mathbb{A}}^\times$ we get $\nu\big(h(\varphi^*(b))\big) = N_{K^*/\mathbb{Q}}(b)$ and $h\big(\varphi^*(b)^{-1}\big) \in G_{\mathbb{A}+}$ ([8, p.172]).

Proposition 4.2 (Shimura's reciprocity law). *Let K, h, z_0 and K^* be as above. Then for every $f \in \mathfrak{A}_0(\mathbb{Q}_{ab})$ which is finite at z_0, the value $f(z_0)$ belongs to K_{ab}^*. Moreover, if $b \in (K^*)_{\mathbb{A}}^\times$, then $f^{h(\varphi^*(b)^{-1})}$ is finite at z_0 and*

$$f(z_0)^{[b,K^*]} = f^{h(\varphi^*(b)^{-1})}(z_0).$$

Proof. [8, Theorem 26.8]. □

5 Class fields over cyclotomic fields

We let ℓ and p be odd prime numbers. We also write for simplicity $\zeta = \zeta_\ell$. Set $k = \mathbb{Q}(\zeta)$ and $n = \frac{\ell-1}{2}$ so that $2n = [k : \mathbb{Q}]$. For $1 \leq i \leq 2n$ we denote by φ_i the element of $\mathrm{Gal}(k/\mathbb{Q})$ defined by $\varphi_i(\zeta) = \zeta^i$. Then $(k; \{\varphi_1, \varphi_2, \ldots, \varphi_n\})$ is a primitive CM-type and $(k; \{\varphi_1^{-1}, \varphi_2^{-1}, \ldots, \varphi_n^{-1}\})$ is its reflex ([8, p.64]). For a positive integer μ, put $S_\mu = \{a \in k^\times \mid a \equiv 1 \pmod{2p^\mu}\}$ and $\widetilde{S_\mu} = \{(a) \mid a \in S_\mu\}$ where (a) is the principal ideal of k generated by a. Let E be the unit group of k and let k_μ be the ray class field of k modulo $2p^\mu$. Then we have

$$\mathrm{Gal}(k_{\mu+1}/k_\mu) \cong \widetilde{S_\mu}/\widetilde{S_{\mu+1}} \cong S_\mu E/S_{\mu+1}E \cong S_\mu/S_{\mu+1}(S_\mu \cap E)$$

by class field theory. Further, we let $H_\mu = S_{\mu+1}(S_\mu \cap E)$ and

$$\omega_{\mu,i} = \begin{cases} 1 + 2p^\mu \zeta^i & \text{for } 1 \leq i \leq n+1 \\ 1 + 2p^\mu(\zeta^n + \zeta^{n+1} - \zeta^i - \zeta^{-i}) & \text{for } n+2 \leq i \leq 2n. \end{cases}$$

Since the ring of integers $\mathcal{O}_k$ of k is equal to $\mathbb{Z}[\zeta]$ and $S_\mu/S_{\mu+1}$ is isomorphic to $\mathcal{O}_k/p\mathcal{O}_k$ by a mapping

$$\begin{aligned} S_\mu/S_{\mu+1} &\longrightarrow \mathcal{O}_k/p\mathcal{O}_k \\ (1 + 2p^\mu\omega)S_{\mu+1} &\longmapsto \omega + p\mathcal{O}_k \quad \text{for } \omega \in \mathcal{O}_k, \end{aligned}$$

we obtain $S_\mu/S_{\mu+1} \cong (\mathbb{Z}/p\mathbb{Z})^{2n}$ and

$$S_\mu/S_{\mu+1} = \langle (1 + 2p^\mu\zeta)S_\mu, (1 + 2p^\mu\zeta^2)S_\mu, \ldots, (1 + 2p^\mu\zeta^{2n})S_\mu \rangle.$$

Let $B = (b_{ij}) \in M_{2n}(\mathbb{Z})$ where b_{ij} is an integer such that $\omega_{\mu,i} = 1 + 2p^\mu\big(\sum_{j=1}^{2n} b_{ij}\zeta^j\big)$. Then we get

$$B = \left(\begin{array}{ccccc|cccc} 1 & & & & & 0 & 0 & \cdots & 0 \\ & 1 & & & & \vdots & \vdots & & \vdots \\ & & \ddots & & & \vdots & \vdots & & \vdots \\ & & & & 1 & 0 & 0 & \cdots & 0 \\ \hline & & & & 0 & 1 & & & \\ & & & -1 & 1 & 1 & -1 & & \\ & & \iddots & & \vdots & \vdots & & \ddots & \\ -1 & & & & 1 & 1 & & & -1 \end{array}\right).$$

Hence, $S_\mu/S_{\mu+1} = \langle \omega_{\mu,1}S_{\mu+1}, \omega_{\mu,2}S_{\mu+1}, \ldots, \omega_{\mu,2n}S_{\mu+1} \rangle$ because $\det(B) = (-1)^{n-1}$ is prime to p. This shows that $S_\mu/H_\mu = \langle \omega_{\mu,1}H_\mu, \omega_{\mu,2}H_\mu, \ldots, \omega_{\mu,2n}H_\mu \rangle$ due to the fact $H_\mu \supset S_{\mu+1}$.

Now, we define an endomorphism φ^* of $k^\times$ by

$$\varphi^*(a) = \prod_{i=1}^{n} a^{\varphi_i^{-1}} \quad \text{for } a \in k^\times$$

and an endomorphism φ^+ of k by

$$\varphi^+(a) = \sum_{i=1}^{n} a^{\varphi_i^{-1}} \quad \text{for } a \in k.$$

And, we let

$$\eta_{\mu,i} = \begin{cases} 1 + 2p^\mu \varphi^+(\zeta^i) & \text{for } 1 \le i \le n+1 \\ 1 & \text{for } n+2 \le i \le 2n \end{cases}$$

so that $\varphi^*(\omega_{\mu,i})H_\mu = \eta_{\mu,i}H_\mu$ for all $1 \le i \le 2n$. Since $\varphi^*(H_\mu) \subset H_\mu$, we can define an endomorphism $\widetilde{\varphi_\mu^*}$ of S_μ/H_μ by $\widetilde{\varphi_\mu^*}(aH_\mu) = \varphi^*(a)H_\mu$. If K_μ is the class field of k corresponding to the kernel of $\widetilde{\varphi_\mu^*}$, then we achieve

$$\text{(5.1)} \qquad \mathrm{Gal}(K_\mu/k_\mu) \cong {}^{S_\mu/H_\mu}\!/_{ker(\widetilde{\varphi_\mu^*})} \cong \widetilde{\varphi_\mu^*}(S_\mu/H_\mu) = \langle \eta_{\mu,1}H_\mu, \eta_{\mu,2}H_\mu, \ldots, \eta_{\mu,n+1}H_\mu \rangle.$$

Observe that K_μ is the fixed field of $\left\{ \left(\frac{k_{\mu+1}/k}{(\omega)}\right) \mid \omega H_\mu \in ker(\widetilde{\varphi_\mu^*}) \right\}$ and

$$\mathrm{Gal}(K_\mu/k_\mu) = \left\langle \left(\frac{k_{\mu+1}/k}{(\omega_{\mu,1})}\right), \left(\frac{k_{\mu+1}/k}{(\omega_{\mu,2})}\right), \ldots, \left(\frac{k_{\mu+1}/k}{(\omega_{\mu,n+1})}\right) \right\rangle.$$

Here, $\left(\frac{k_{\mu+1}/k}{\cdot}\right)$ is the Artin map of $k_{\mu+1}/k$.

PROPOSITION 5.1. *Let N be a positive integer, $K = \mathbb{Q}(\zeta_N)$ and K^+ be its maximal real subfield. Let E (resp. E^+) be the unit group of K (resp. K^+) and W be the group of roots of unity in K. Then we have*

$$|E : WE^+| = \begin{cases} 1 & \text{if } N \text{ is a prime power} \\ 2 & \text{if } N \text{ is not a prime power} \end{cases}.$$

PROOF. [11, Corollary 4.13]. □

PROPOSITION 5.2. *Let ℓ be any prime and $m \in \mathbb{N}$. Let $\mathbb{Q}(\zeta_{\ell^m})^+$ be the maximal real subfield of $\mathbb{Q}(\zeta_{\ell^m})$ and $E_{\ell^m}^+$ be its unit group. Further, we let $C_{\ell^m}^+$ be the subgroup of $E_{\ell^m}^+$ generated by -1 and the real units*

$$\xi_a = \zeta_{\ell^m}^{\frac{1-a}{2}} \cdot \frac{1-\zeta_{\ell^m}^a}{1-\zeta_{\ell^m}} \in \mathbb{R}, \quad 1 < a < \frac{1}{2}\ell^m, \quad (a,\ell) = 1.$$

Then

$$h_{\ell^m}^+ = |E_{\ell^m}^+ : C_{\ell^m}^+|,$$

where $h_{\ell^m}^+$ is the class number of $\mathbb{Q}(\zeta_{\ell^m})^+$.

PROOF. [11, Lemma 8.1 and Theorem 8.2]. □

LEMMA 5.3. *Let ℓ be an odd prime and p be an odd prime such that $p \nmid \ell h_\ell^+$, where h_ℓ^+ is the class number of the maximal real subfield of k. Then $H_\mu/S_{\mu+1}$ is generated by real units of k for all $\mu \in \mathbb{N}$.*

PROOF. The $(2\ell h_\ell^+)$-th power mapping of $S_\mu/S_{\mu+1}$ induces an automorphism of itself because $(p, 2\ell h_\ell^+) = 1$. Thus the image of $E \cap S_\mu$ in $S_\mu/S_{\mu+1}$ is the same as that of $E^{2\ell h_\ell^+} \cap S_\mu$. By Proposition 5.1 and 5.2, $E^{2\ell h_\ell^+} \subset \langle \xi_a^{2\ell} \mid 1 < a < \frac{\ell}{2} \rangle$ where $\xi_a = \zeta^{\frac{1-a}{2}} \cdot \frac{1-\zeta^a}{1-\zeta} \in \mathbb{R}$. Therefore $H_\mu/S_{\mu+1} = S_{\mu+1}(E^{2\ell h_\ell^+} \cap S_\mu)/S_{\mu+1}$ is generated by real units of k. □

Let $M_\ell(p) = (m_{ij}) \in M_{(n+1)\times 2n}(\mathbb{Z}/p\mathbb{Z})$ where m_{ij} is the coefficient of ζ^j in $\varphi^+(\zeta^i)$ in $\mathbb{Z}/p\mathbb{Z}$. Then we get

$$m_{ij} = \begin{cases} 1 & \text{if } \ \overline{i} \cdot \overline{j}^{\,-1} \in \{\overline{1}, \overline{2}, \ldots, \overline{n}\} \text{ in } \mathbb{Z}/\ell\mathbb{Z} \\ 0 & \text{otherwise.} \end{cases}$$

We can then easily see that the rank of $M_\ell(p)$ is equal to the dimension of the vector subspace $\langle \eta_{\mu,1} S_{\mu+1}, \eta_{\mu,2} S_{\mu+1}, \ldots, \eta_{\mu,n+1} S_{\mu+1} \rangle$ in $S_\mu/S_{\mu+1}$.

LEMMA 5.4. *Let ℓ and p be odd primes and $\mu \in \mathbb{N}$. For $1 \le i, j \le 2n$, let*

$$n_{ij} = \begin{cases} 1 & \textit{if } \ \overline{i} \cdot \overline{j} \in \{\overline{1}, \overline{2}, \ldots, \overline{n}\} \textit{ in } \mathbb{Z}/\ell\mathbb{Z} \\ 0 & \textit{otherwise} \end{cases}$$

and let $N_\ell = \big(n_{ij}\big)_{1 \le i,j \le n} \in M_n(\mathbb{Z})$. Then the images $\eta_{\mu,1}, \eta_{\mu,2}, \ldots, \eta_{\mu,n+1}$ are linearly independent in $S_\mu/S_{\mu+1}$ if and only if $p \nmid \det(N_\ell)$.

PROOF. Let $N_\ell' = \big(n_{ij}\big)_{\substack{1 \le i \le n+1 \\ 1 \le j \le 2n}} \in M_{(n+1)\times 2n}(\mathbb{Z}/p\mathbb{Z})$. It is clear that $\operatorname{rank}\big(M_\ell(p)\big) = \operatorname{rank}(N_\ell')$. Hence the images $\eta_{\mu,1}, \eta_{\mu,2}, \ldots, \eta_{\mu,n+1}$ are linearly independent in $S_\mu/S_{\mu+1}$ if and only if N_ℓ' has rank $n+1$. Now, we claim that $\operatorname{rank}(N_\ell') = n+1$ if and only if N_ℓ' induces the following row echelon form

$$\begin{pmatrix} 1 & & & & & & & -1 \\ & 1 & & & & & -1 & \\ & & \ddots & & & \iddots & & \\ & & & & 1 & -1 & & \\ & & & & & 1 \quad 1 & \cdots & 1 \end{pmatrix}. \tag{5.2}$$

The "if" part is obvious. Note that if $n_{ij} = 1$ (resp. 0), then $n_{i\ \ell-j} = 0$ (resp. 1) because there are no two automorphisms among $\varphi_1, \varphi_2, \ldots, \varphi_n$ which are complex conjugate of each other. Let v_i be the ith row vector of N_ℓ' for $1 \le i \le n+1$ and let

$$v_i' = \big(v_{ij}'\big)_{1 \le j \le 2n} = \begin{cases} 2v_i - v_n - v_{n+1} & \text{for } \ 1 \le i \le n \\ v_n + v_{n+1} & \text{for } i = n+1. \end{cases}$$

Observe that $v'_{n+1} = (1 \ \ 1 \ \ \cdots \ \ 1)$ and $2 \in (\mathbb{Z}/p\mathbb{Z})^\times$. For $1 \le i \le n$, if $v'_{ij} = 1$ (resp. -1) then $v_{i\ \ell-j} = -1$ (resp. 1). Thus we can write v'_i as a linear combination of the row vectors of the above row echelon form (5.2), and hence the claim is proved. By the above claim $\mathrm{rank}(N'_\ell) = n+1$ if and only if $\det\Big(\big(n_{ij}\big)_{1\le i,j\le n+1}\Big) \not\equiv 0 \pmod{p}$. Since

$$\big(-n_{1j} + n_{nj} + n_{n+1\ j}\big)_{1\le j\le n+1} = (0 \ \ 0 \ \ \cdots \ \ 0 \ \ 1),$$

we derive

$$\det\Big(\big(n_{ij}\big)_{1\le i,j\le n+1}\Big) = \det(N_\ell).$$

This completes the proof. □

THEOREM 5.5. *Let ℓ and p be odd primes and put $n = \frac{\ell-1}{2}$. Further, let $M_\ell(p)$ and N_ℓ be as above. If $p \nmid \ell h^+_\ell n$, then for every $\mu \in \mathbb{N}$ we deduce*

$$\mathrm{Gal}(K_\mu/k_\mu) \cong (\mathbb{Z}/p\mathbb{Z})^{rank(M_\ell(p))}.$$

And, if $p \nmid \det(N_\ell)$, then we obtain

$$\mathrm{Gal}(K_\mu/k_\mu) \cong (\mathbb{Z}/p\mathbb{Z})^{n+1}.$$

PROOF. By (5.1) it suffices to show that the dimension of $\langle \eta_{\mu,1}S_{\mu+1}, \eta_{\mu,2}S_{\mu+1}, \ldots, \eta_{\mu,n+1}S_{\mu+1}\rangle$ in $S_\mu/S_{\mu+1}$ is equal to the dimension of $\langle \eta_{\mu,1}H_\mu, \eta_{\mu,2}H_\mu, \ldots, \eta_{\mu,n+1}H_\mu\rangle$ in S_μ/H_μ. If $n = 1$, then $H_\mu = S_{\mu+1}$ by Lemma 5.3; hence we are done in this case. Thus we may assume $n \ge 2$. It is well known that $\mathbb{Z}[\zeta+\zeta^{-1}]$ is the ring of integers of the maximal real subfield $\mathbb{Q}(\zeta+\zeta^{-1})$ of k and $[\mathbb{Q}(\zeta+\zeta^{-1}) : \mathbb{Q}] = n$ ([6, Theorem 4]). Therefore, if $uS_{\mu+1} \in H_\mu/S_{\mu+1}$, then by Lemma 5.3 we can write

$$u = 1 + 2p^\mu\big(a_0 + a_1(\zeta+\zeta^{-1}) + a_2(\zeta+\zeta^{-1})^2 + \cdots + a_{n-1}(\zeta+\zeta^{-1})^{n-1}\big) \in S_\mu \cap E$$

for some $a_i \in \mathbb{Z}$ with $0 \le i \le n-1$. If $p \mid a_i$ for $1 \le i \le n-1$, then

$$\begin{aligned} N_{\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}}(u) &\equiv 1 + 2p^\mu n a_0 \pmod{2p^{\mu+1}} \\ &= 1. \end{aligned}$$

Since $p \nmid n$, we have $p \mid a_0$ and so $u \in S_{\mu+1}$.

Now, we set

$$\begin{aligned} b &= a_0 + a_1(\zeta+\zeta^{-1}) + a_2(\zeta+\zeta^{-1})^2 + \cdots + a_{n-1}(\zeta+\zeta^{-1})^{n-1} \\ &= b_0 + b_1\zeta + b_2\zeta^2 + \cdots + b_n\zeta^n + b_n\zeta^{-n} + b_{n-1}\zeta^{-(n-1)} + \cdots + b_1\zeta^{-1}, \end{aligned}$$

where $b_i \in \mathbb{Z}$ for $0 \leq i \leq n$. Observe that $b_n = 0$, $b_{n-1} = a_{n-1}$ and $b_{n-2} = a_{n-2}$. Consider the following matrix

$$\mathbf{M} = \begin{pmatrix} 1 & & & & & & & -1 \\ & 1 & & & & & -1 & \\ & & \ddots & & & \iddots & & \\ & & & 1 & -1 & & & \\ & & & & 1 & 1 & \cdots & 1 \\ b_1 - b_0 & b_2 - b_0 & \cdots & b_n - b_0 & b_n - b_0 & \cdots & b_2 - b_0 & b_1 - b_0 \end{pmatrix} \in M_{(n+2)\times 2n}(\mathbb{Z}/p\mathbb{Z}).$$

The last row of $\mathbf{M}$ is induced from the coefficients of ζ^j for $1 \leq j \leq 2n$ in b. So, $\mathbf{M}$ is row equivalent to

$$\begin{aligned} \mathbf{M} &\sim \begin{pmatrix} 1 & & & & & & & -1 \\ & 1 & & & & & -1 & \\ & & \ddots & & & \iddots & & \\ & & & 1 & -1 & & & \\ & & & & 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 & 2(b_n - b_0) & 2(b_{n-1} - b_0) & \cdots & 2(b_1 - b_0) \end{pmatrix} \\ &\sim \begin{pmatrix} 1 & & & & & & -1 \\ & 1 & & & & -1 & \\ & & \ddots & & \iddots & & \\ & & & 1 & -1 & & \\ & & & & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 & 2b_{n-1} & \cdots & 2b_1 \end{pmatrix} \quad \text{because } b_n = 0. \end{aligned}$$

Here we claim that if $u \notin S_{\mu+1}$, then the rank of $\mathbf{M}$ is $n+2$. Indeed, if $p \nmid a_{n-1}$ or $p \nmid a_{n-2}$ then we are done. Otherwise, we get

$$\begin{aligned} b_{n-3} &\equiv a_{n-3} \pmod{p} \\ b_{n-4} &\equiv a_{n-4} \pmod{p}. \end{aligned}$$

Hence by induction we ensure that the rank of $\mathbf{M}$ is $n+1$ if and only if $p \mid a_i$ for all $1 \leq i \leq n-1$. Since $u \notin S_{\mu+1}$, we obtain $p \nmid a_i$ for some $1 \leq i \leq n-1$, and the claim is proved. In the proof of Lemma 5.4 we already showed that every row vector of $M_\ell(p)$ can be written as a linear combination of the row vectors of the matrix (5.2). Therefore, if $u \notin S_{\mu+1}$ then by the above claim for each $1 \leq i \leq n+1$ the images of $\eta_{\mu,i}$ and u in $S_\mu/S_{\mu+1}$ are linearly independent, as desired. Furthermore if $p \nmid \det(N_\ell)$, then by Lemma 5.4 we achieve $\operatorname{rank}\big(M_\ell(p)\big) = n+1$. $\square$

COROLLARY 5.6. *Suppose $p \nmid \ell h_\ell^+ n$. Then K_μ becomes the ray class field $k_{\mu+1}$ for all $\mu \in \mathbb{N}$ if and only if $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = n-1$ and $p \nmid \det(N_\ell)$.*

PROOF. Suppose that $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = n-1$ and $p \nmid \det(N_\ell)$. We claim that $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_\mu/S_{\mu+1}) = n-1$ for all $\mu \in \mathbb{N}$. Indeed, let $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n-1}$ be elements of $S_1 \cap E$ whose images form a basis for H_1/S_2. Since $\varepsilon_i^p \in H_2 - S_3$ for all i, the images $\varepsilon_1^p, \varepsilon_2^p, \ldots, \varepsilon_{n-1}^p$ turn out to be a basis for H_2/S_3. And by induction the claim is proved. By Theorem 5.5 and the assumptions, we deduce

$$\begin{aligned} |\mathrm{Gal}(K_\mu/k_\mu)| &= |\widetilde{\varphi_\mu^*}(S_\mu/H_\mu)| = p^{n+1}, \\ |\mathrm{Gal}(k_{\mu+1}/k_\mu)| &= |S_\mu/H_\mu| = \frac{|S_\mu/S_{\mu+1}|}{|H_\mu/S_{\mu+1}|} = p^{n+1}. \end{aligned}$$

Therefore $K_\mu = k_{\mu+1}$ because $K_\mu \subset k_{\mu+1}$.

Conversely, suppose that $K_\mu = k_{\mu+1}$ for all $\mu \in \mathbb{N}$. It follows from the proof of Lemma 5.3 that $|H_\mu/S_{\mu+1}| \le p^{n-1}$, and so $|\mathrm{Gal}(k_{\mu+1}/k_\mu)| \ge p^{n+1}$. On the other hand, $|\mathrm{Gal}(K_\mu/k_\mu)| \le p^{n+1}$ by the formula (5.1). Since $K_\mu = k_{\mu+1}$, we have $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = n-1$ and $|\mathrm{Gal}(K_\mu/k_\mu)| = p^{n+1}$; hence $p \nmid \det(N_\ell)$ by Lemma 5.4 and Theorem 5.5. □

REMARK 5.7. (i) We are able to show that $\det(N_\ell) \neq 0$ for $\ell \le 8000$ with an aid of computer computation, from which we conjecture that $\det(N_\ell) \neq 0$ holds for all odd primes ℓ.

(ii) Let $\xi_a = \zeta^{\frac{1-a}{2}} \cdot \frac{1-\zeta^a}{1-\zeta} \in \mathbb{R}$ for $1 < a < \frac{\ell}{2}$. When $\ell = 5$, we obtain

$$\begin{aligned} \xi_2^{48} &\equiv 1 \pmod{14} \\ &\not\equiv 1 \pmod{98}. \end{aligned}$$

Thus $\dim_{\mathbb{Z}/7\mathbb{Z}}(H_1/S_2) = 1$, and Corollary 5.6 holds for $p = 7$. In a similar way, we can show that $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = 1$ holds for all odd primes $p \le 101$ except $p = 3$. When $\ell = 7$, we see that $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = 2$ holds for all odd primes $p \le 101$. So, we also conjecture that for each odd prime ℓ, $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = n-1$ holds for almost all odd primes p. If the above two conjectures are true, then we have the isomorphism

$$\mathrm{Gal}(k_{\mu+1}/k_\mu) \cong (\mathbb{Z}/p\mathbb{Z})^{n+1}$$

for each odd prime ℓ and almost all odd primes p.

(iii) The following table gives rise to the generators of H_1/S_2 for $\ell = 5, 7$.

p	generators of H_1/S_2	
	ℓ=5	ℓ=7
3	1	ξ_2^{182}, ξ_3^{182}
5	ξ_2^{60}	ξ_2^{868}, ξ_3^{868}
7	ξ_2^{48}	ξ_2^{42}, ξ_3^{42}
11	ξ_2^{30}	$\xi_2^{1330}, \xi_3^{1330}$
13	ξ_2^{84}	ξ_2^{84}, ξ_3^{84}
17	ξ_2^{72}	$\xi_2^{17192}, \xi_3^{34384}$
19	ξ_2^{18}	$\xi_2^{16002}, \xi_3^{16002}$
23	ξ_2^{528}	$\xi_2^{12166}, \xi_3^{12166}$
29	ξ_2^{848}	ξ_2^{28}, ξ_3^{28}
31	ξ_2^{30}	$\xi_2^{69510}, \xi_3^{69510}$
37	ξ_2^{684}	$\xi_2^{16884}, \xi_3^{16884}$
41	ξ_2^{120}	ξ_2^{280}, ξ_3^{280}
43	ξ_2^{1848}	ξ_2^{42}, ξ_3^{42}

p	generators of H_1/S_2	
	ℓ=5	ℓ=7
47	ξ_2^{2208}	$\xi_2^{726754}, \xi_3^{726754}$
53	ξ_2^{1404}	$\xi_2^{148876}, \xi_3^{148876}$
59	ξ_2^{174}	$\xi_2^{1437646}, \xi_3^{1437646}$
61	ξ_2^{60}	$\xi_2^{40740}, \xi_3^{40740}$
67	ξ_2^{4488}	$\xi_2^{100254}, \xi_3^{100254}$
71	ξ_2^{210}	ξ_2^{70}, ξ_3^{70}
73	ξ_2^{1332}	$\xi_2^{226926}, \xi_3^{453852}$
79	ξ_2^{78}	$\xi_2^{164346}, \xi_3^{164346}$
83	ξ_2^{6888}	ξ_2^{574}, ξ_3^{574}
89	ξ_2^{132}	$\xi_2^{1233694}, \xi_3^{4934776}$
97	ξ_2^{2352}	ξ_2^{672}, ξ_3^{672}
101	ξ_2^{300}	$\xi_2^{7212100}, \xi_3^{7212100}$

6 Construction of class fields

We use the same notations as in Section 5. Let $k = \mathbb{Q}(\zeta)$ with $\zeta = \zeta_\ell$ and $n = \frac{\ell-1}{2}$ so that $2n = [k : \mathbb{Q}]$. Let $v : k \to \mathbb{C}^n$ be the map given by $v(\alpha) = \begin{pmatrix} \alpha^{\varphi_1} \\ \vdots \\ \alpha^{\varphi_1} \end{pmatrix}$, $L = v(\mathcal{O}_k)$ be a lattice in $\mathbb{C}^n$ and $\rho = \frac{\zeta-\zeta^{-1}}{\ell} \in k$. Then ρ satisfies the conditions (i)$\sim$(iv) in §4. And, we have an $\mathbb{R}$-bilinear form $E : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{R}$ defined by

$$E(z,w) = \sum_{i=1}^{n} \rho^{\varphi_i}(z_i\overline{w_i} - \overline{z_i}w_i) \quad \text{for } z = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix},\ w = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix},$$

which induces a non-degenerate Riemann form on $\mathbb{C}^n/L$. Let

$$e_i = \begin{cases} \zeta^{2i} & \text{for } 1 \le i \le n \\ \displaystyle\sum_{j=1}^{i-n} \zeta^{2j-1} & \text{for } n+1 \le i \le 2n. \end{cases}$$

Since $\{e_1, e_2, \ldots, e_{2n}\}$ is a free $\mathbb{Z}$-basis of $\mathcal{O}_k$, $\{v(e_1), v(e_2), \ldots, v(e_{2n})\}$ is a free $\mathbb{Z}$-basis of the lattice L, and we get

$$\Big(E\big(v(e_i), v(e_j)\big)\Big)_{1 \le i,j \le 2n} = J.$$

Now, let

$$\Omega = \begin{pmatrix} v(e_1) & v(e_2) & \cdots & v(e_{2n}) \end{pmatrix} \in M_{n\times 2n}(\mathbb{C}).$$

Then Ω satisfies

$$\begin{aligned} L &= \left\{ \Omega \begin{pmatrix} a \\ b \end{pmatrix} \mid a, b \in \mathbb{Z}^n \right\}, \\ E(\Omega x, \Omega y) &= {}^t x J y \quad \text{for } (x, y) \in \mathbb{R}^{2n} \times \mathbb{R}^{2n} \end{aligned}$$

because E is $\mathbb{R}$-bilinear. Thus $\delta = 1$ and $\epsilon = 1_n$ in §4. Write $\Omega = (\Omega_1 \quad \Omega_2)$ with $\Omega_1, \Omega_2 \in M_n(\mathbb{C})$ and put $z_\ell = \Omega_2^{-1}\Omega_1 \in \mathbb{H}_n$. We define a ring monomorphism h of $k_{\mathbb{A}}$ into $M_{2n}(\mathbb{Q}_{\mathbb{A}})$ as in §4. Then z_ℓ is the CM-point of $\mathbb{H}_n$ induced from h corresponding to the polarized abelian variety $(\mathbb{C}^n/L, E)$ which is in fact a polarized Jacobian variety of the curve $y^2 = 1 - x^\ell$ ([8, p.113]).

Let p be an odd prime and $r, s \in \mathbb{Q}^n$. We denote by $\mathbf{h}$ the set of all non-archimedean primes of k and by $\mathbf{a}$ the set of all archimedean primes of k. For given $\omega \in \mathcal{O}_k$ prime to $2p$, we set

$$\widetilde{\omega} = \prod_{\substack{v\in\mathbf{h} \\ v \mid 2p}} (\omega^{-1})_v \times \prod_{\substack{v\in\mathbf{h} \\ v \nmid 2p}} 1_v \times \prod_{v\in\mathbf{a}} 1_v \in k_{\mathbb{A}}^\times.$$

Here x_v is the v-component of $x \in k_{\mathbb{A}}^\times$. If $\Phi_{(r,s)}$ is finite at z_ℓ then by Proposition 4.2 and [5, Chapter 8 §4], we obtain

$$\Phi_{(r,s)}(z_\ell)^{\left(\frac{k'/k}{(\omega)}\right)} = \Phi_{(r,s)}(z_\ell)^{[\widetilde{\omega},k]} = \left(\Phi_{(r,s)}\right)^{h(\varphi^*(\widetilde{\omega}^{-1}))}(z_\ell) \quad \text{for } \omega \in \mathcal{O}_k,$$

where k' is a finite abelian extension of k containing $\Phi_{(r,s)}(z_\ell)$.

Lemma 6.1. *Let p be an odd prime, $\mu \in \mathbb{N}$, $r, s \in \frac{1}{p^\mu}\mathbb{Z}^n$ and z_ℓ be as above. Assume that z_ℓ is not a zero of $\Theta(0, z; 0, 0)$. If $p \nmid \ell h_\ell^+ n$, then $\Phi_{(r,s)}(z_\ell)^{p^\alpha} \in K_{2\mu-1-\alpha}$ for $0 \le \alpha \le \mu$.*

Proof. By Proposition 3.5 and [7, p.682], $\Phi_{(r,s)}(z)$ belongs to $\mathfrak{A}_0\big(\Gamma(2p^{2\mu}), \mathbb{Q}(\zeta_{2p^{2\mu}})\big)$ as a function, so it is $R_{2p^{2\mu}}$-invariant. Let $\omega H_{2\mu-1-\alpha} \in \ker(\widetilde{\varphi^*_{2\mu-1-\alpha}})$ such that $\varphi^*(\omega) \in H_{2\mu-1-\alpha}$. Since $p \nmid \ell h_\ell^+ n$, from the proof of Theorem 5.5 we get that $(\varphi^*(S_{2\mu-1-\alpha}) \cap H_{2\mu-1-\alpha})/S_{2\mu-\alpha} = \{0\}$. Hence $\varphi^*(\omega) \in S_{2\mu-\alpha}$. Write $\varphi^*(\omega) = 1 + 2p^{2\mu-\alpha}\omega_0$ with $\omega_0 \in \mathcal{O}_k$. Then it suffices to show that $\big(\Phi_{(r,s)}(z_\ell)^{p^\alpha}\big)^{\left(\frac{k'/k}{(\omega)}\right)} = \Phi_{(r,s)}(z_\ell)^{p^\alpha}$. By the strong approximation theorem for $Sp(n)$ there exists a matrix $\beta \in \Gamma(1)$ such that

$$h\big(\varphi^*(\omega)\big) \equiv \begin{pmatrix} 1_n & 0 \\ 0 & v \cdot 1_n \end{pmatrix} \beta \pmod{2p^{2\mu}},$$

where $v := \nu\big(h(\varphi^*(\omega))\big) = N_{k/\mathbb{Q}}(\omega) = \varphi^*(\omega) \cdot \overline{\varphi^*(\omega)} = 1 + 2p^{2\mu-\alpha}v_0$ for some $v_0 \in \mathbb{Z}$. In fact, β belongs to $\Gamma(2)$ owing to the facts $h\big(\varphi^*(\omega)\big) \equiv 1_{2n} \pmod 2$ and $v \equiv 1 \pmod 2$.

Thus for all rational primes q we obtain

$$h\big(\varphi^*(\widetilde{\omega}^{-1})\big)_q \equiv \begin{pmatrix} 1_n & 0 \\ 0 & v\cdot 1_n \end{pmatrix}\beta \pmod{2p^{2\mu}M_{2n}(\mathbb{Z}_q)}.$$

And, by Lemma 3.4 and Corollary 3.6 we get that

$$\begin{aligned}\big(\Phi_{(r,s)}\big)^{h(\varphi^*(\widetilde{\omega}^{-1}))}(z_\ell) &= \Phi_{(r,vs)}(\beta z_\ell)\\ &= e\Big(\frac{{}^trvs - {}^tr's'}{2}\Big)\Phi_{(r',s')}(z_\ell),\end{aligned}$$

where

$$\begin{aligned}\begin{pmatrix} r' \\ s' \end{pmatrix} = {}^t\beta\begin{pmatrix} r \\ vs \end{pmatrix} &\equiv {}^th\big(\varphi^*(\omega)\big)\begin{pmatrix} r \\ s \end{pmatrix}\\ &\equiv \begin{pmatrix} r \\ s \end{pmatrix} + 2p^{2\mu-\alpha}\cdot {}^th(\omega_0)\begin{pmatrix} r \\ s \end{pmatrix} \pmod{2p^{2\mu}}.\end{aligned}$$

Let $a, b \in 2p^{\mu-\alpha}\mathbb{Z}^n \subset 2\mathbb{Z}^n$ such that $\begin{pmatrix} a \\ b \end{pmatrix} = 2p^{2\mu-\alpha}\cdot {}^th(\omega_0)\begin{pmatrix} r \\ s \end{pmatrix}$. Then by Lemma 3.4 and Proposition 4.2 we derive that

$$\begin{aligned}\big(\Phi_{(r,s)}(z_\ell)^{p^\alpha}\big)^{\left(\frac{k'/k}{(\omega)}\right)} &= \big(\Phi_{(r,s)}{}^{h(\varphi^*(\widetilde{\omega}^{-1}))}(z_\ell)\big)^{p^\alpha}\\ &= \Big(e\big(\tfrac{{}^trvs - {}^t(r+a)(s+b)}{2}\big)e\big({}^trb\big)\Phi_{(r,s)}(z_\ell)\Big)^{p^\alpha}\\ &= e(p^{2\mu}v_0\cdot {}^trs)e\Big(p^\alpha\cdot\tfrac{{}^trb - {}^tas}{2}\Big)\Phi_{(r,s)}(z_\ell)^{p^\alpha}\\ &= \Phi_{(r,s)}(z_\ell)^{p^\alpha}.\end{aligned}$$

□

Let $\mu \in \mathbb{N}$. Assume that $r, s \in \frac{1}{p^\mu}\mathbb{Z}^n$ and z_ℓ is not a zero of $\Theta(0, z; 0, 0)$. Consider the matrices $h\big(\varphi^*(\omega_{2\mu-1-\alpha,j})\big)$ for $1 \le j \le n+1$ and $0 \le \alpha \le \mu-1$. Then we achieve

$$\begin{aligned}h\big(\varphi^*(\omega_{2\mu-1-\alpha,j})\big) &= h\big(1 + 2p^{2\mu-1-\alpha}\varphi^+(\zeta^j) + 2p^{2\mu-\alpha}\omega_0\big)\\ &= 1_{2n} + 2p^{2\mu-1-\alpha}h\big(\varphi^+(\zeta^j)\big) + 2p^{2\mu-\alpha}h(\omega_0)\end{aligned}$$

for some $\omega_0 \in \mathcal{O}_k$. Also, we can deduce without difficulty

$$h(\zeta) = \left(\begin{array}{ccccc|ccccc} 0 & 0 & \cdots & \cdots & 0 & -1 & 1 & & & \\ \vdots & \vdots & & & \vdots & & -1 & 1 & & \\ \vdots & \vdots & & & \vdots & & & \ddots & \ddots & \\ 0 & 0 & \cdots & \cdots & 0 & & & & -1 & 1 \\ -1 & -1 & \cdots & \cdots & -1 & & & & & -1 \\ \hline 1 & & & & & 0 & 0 & \cdots & \cdots & 0 \\ 1 & 1 & & & & \vdots & \vdots & & & \vdots \\ 1 & 1 & 1 & & & \vdots & \vdots & & & \vdots \\ \vdots & \vdots & & \ddots & & \vdots & \vdots & & & \vdots \\ 1 & 1 & 1 & \cdots & 1 & 0 & 0 & \cdots & \cdots & 0 \end{array}\right).$$

Now, again by the strong approximation theorem for $Sp(n)$ there exists a matrix $\beta_{2\mu-1-\alpha,j} \in \Gamma(1)$ such that

$$h\big(\varphi^*(\omega_{2\mu-1-\alpha,j})\big) \equiv \begin{pmatrix} 1_n & 0 \\ 0 & v_{2\mu-1-\alpha,j} \cdot 1_n \end{pmatrix} \beta_{2\mu-1-\alpha,j} \pmod{2p^{2\mu}},$$

where $v_{2\mu-1-\alpha,j} := \nu\big(h(\varphi^*(\omega_{2\mu-1-\alpha,j}))\big) = N_{k/\mathbb{Q}}(\omega_{2\mu-1-\alpha,j}) = 1 - 2p^{2\mu-1-\alpha} + 2p^{2\mu-\alpha}v_j$ for some $v_j \in \mathbb{Z}$. In fact, $\beta_{2\mu-1-\alpha,j}$ belongs to $\Gamma(2)$ due to the facts $h\big(\varphi^*(\omega_{2\mu-1-\alpha,j})\big) \equiv 1_{2n} \pmod 2$ and $v_{2\mu-1-\alpha,j} \equiv 1 \pmod 2$. Thus for all rational primes q we obtain

$$h\big(\varphi^*(\widetilde{\omega}^{-1}_{2\mu-1-\alpha,j})\big)_q \equiv \begin{pmatrix} 1_n & 0 \\ 0 & v_{2\mu-1-\alpha,j} \cdot 1_n \end{pmatrix} \beta_{2\mu-1-\alpha,j} \pmod{2p^{2\mu} M_{2n}(\mathbb{Z}_q)}.$$

By Lemma 3.4 and Corollary 3.6 we get that

$$\begin{aligned} \Phi_{(r,s)}{}^{h(\varphi^*(\widetilde{\omega}^{-1}_{2\mu-1-\alpha,j}))}(z_\ell) &= \Phi_{(r,v_{2\mu-1-\alpha,j}s)}(\beta_{2\mu-1-\alpha,j}(z_\ell)) \\ &= e\Big(\frac{{}^t r v_{2\mu-1-\alpha,j} s - {}^t r' s'}{2}\Big)\Phi_{(r',s')}(z_\ell), \end{aligned}$$

where

$$\begin{aligned} \begin{pmatrix} r' \\ s' \end{pmatrix} &= {}^t\beta_{2\mu-1-\alpha,j} \begin{pmatrix} r \\ v_{2\mu-1-\alpha,j} s \end{pmatrix} \equiv {}^t h\big(\varphi^*(\omega_{2\mu-1-\alpha,j})\big) \begin{pmatrix} r \\ s \end{pmatrix} \\ &\equiv \begin{pmatrix} r \\ s \end{pmatrix} + 2p^{2\mu-1-\alpha} \cdot {}^t h\big(\varphi^+(\zeta^j)\big) \begin{pmatrix} r \\ s \end{pmatrix} + 2p^{2\mu-\alpha} \cdot {}^t h(\omega_0) \begin{pmatrix} r \\ s \end{pmatrix} \pmod{2p^{2\mu}}. \end{aligned}$$

For each j, let $a_{2\mu-1-\alpha,j}, b_{2\mu-1-\alpha,j} \in 2p^{\mu-1-\alpha}\mathbb{Z}^n \subset 2\mathbb{Z}^n$ such that

$$\begin{pmatrix} a_{2\mu-1-\alpha,j} \\ b_{2\mu-1-\alpha,j} \end{pmatrix} = 2p^{2\mu-1-\alpha} \cdot {}^t h\big(\varphi^+(\zeta^j)\big) \begin{pmatrix} r \\ s \end{pmatrix}.$$

And, let $c, d \in 2p^{\mu-\alpha}\mathbb{Z}^n \subset 2\mathbb{Z}^n$ such that $\begin{pmatrix} c \\ d \end{pmatrix} = 2p^{2\mu-\alpha} \cdot {}^t h(\omega_0) \begin{pmatrix} r \\ s \end{pmatrix}$. Then by Lemma 3.4 and Proposition 4.2 we derive that

(6.1)

$$\begin{aligned}
\big(\Phi_{(r,s)}(z_\ell)^{p^\alpha}\big)^{\left(\frac{K_{2\mu-1-\alpha}/k}{(\omega_{2\mu-1-\alpha,j})}\right)} &= \big(\Phi_{(r,s)}{}^{h(\varphi^*(\widetilde{\omega}_{2\mu-1-\alpha,j}^{-1}))}(z_\ell)\big)^{p^\alpha} \\
&= \Big(e\big(\tfrac{{}^t r v_{2\mu-1-\alpha,j} s - {}^t(r+a_{2\mu-1-\alpha,j}+c)(s+b_{2\mu-1-\alpha,j}+d)}{2}\big) e\big({}^t r(b_{2\mu-1-\alpha,j}+d)\big)\Phi_{(r,s)}(z_\ell)\Big)^{p^\alpha} \\
&= e(-p^{2\mu-1} \cdot {}^t r s) e\Big(p^\alpha \tfrac{{}^t r b_{2\mu-1-\alpha,j} - {}^t a_{2\mu-1-\alpha,j} s}{2}\Big) \Phi_{(r,s)}(z_\ell)^{p^\alpha} \\
&= \underbrace{e(-p^{2\mu-1} \cdot {}^t r s) e\Big(\frac{{}^t r b_{2\mu-1,j} - {}^t a_{2\mu-1,j} s}{2}\Big)}_{p\text{-th root of unity}} \Phi_{(r,s)}(z_\ell)^{p^\alpha}.
\end{aligned}$$

For given $r_i, s_i \in \mathbb{Z}^n$ with $1 \le i \le n+1$, let $\mathbf{r} = (r_i)_{1\le i\le n+1}$ and $\mathbf{s} = (s_i)_{1\le i\le n+1}$. And, we set $\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z)_p = \Phi_{(\frac{1}{p^\mu} r_i, \frac{1}{p^\mu} s_i)}(z)$ for each $\mu \in \mathbb{N}$.

LEMMA 6.2. *Let $\mathbf{r} = (r_i)_{1\le i\le n+1}$ and $\mathbf{s} = (s_i)_{1\le i\le n+1}$ for given $r_i, s_i \in \mathbb{Z}^n$. Then for each $1 \le i, j \le n+1$, there exists an integer a_{ij} such that $\Phi_{[\mathbf{r},\mathbf{s};1,i]}(z_\ell)_p^{\left(\frac{K_1/k}{(\omega_{1,j})}\right)} = \zeta_p^{a_{ij}} \Phi_{[\mathbf{r},\mathbf{s};1,i]}(z_\ell)_p$ for all odd primes p.*

PROOF. Substituting $r = \frac{1}{p} r_i$, $s = \frac{1}{p} s_i$ into the formula (6.1) we get

$$\begin{aligned}
\Phi_{[\mathbf{r},\mathbf{s};1,i]}(z_\ell)_p^{\left(\frac{K_1/k}{(\omega_{1,j})}\right)} &= e\Big(-\tfrac{{}^t r_i s_i}{p}\Big) e\Big(\tfrac{{}^t r_i b_{1,j} - {}^t a_{1,j} s_i}{2p}\Big) \Phi_{[\mathbf{r},\mathbf{s};1,i]}(z_\ell)_p \\
&= \zeta_p^{-{}^t r_i s_i + \frac{1}{2}({}^t r_i b_{1,j} - {}^t a_{1,j} s_i)} \Phi_{[\mathbf{r},\mathbf{s};1,i]}(z_\ell)_p,
\end{aligned}$$

where $a_{1,j}, b_{1,j} \in 2\mathbb{Z}^n$ such that $\begin{pmatrix} a_{1,j} \\ b_{1,j} \end{pmatrix} = 2 \cdot {}^t h\big(\varphi^+(\zeta^j)\big) \begin{pmatrix} r_i \\ s_i \end{pmatrix}$. Hence $a_{ij} := -{}^t r_i s_i + \frac{1}{2}({}^t r_i b_{1,j} - {}^t a_{1,j} s_i)$ is an integer which does not depend on p. □

We put $A_\ell(\mathbf{r}, \mathbf{s}) = (a_{ij})_{1\le i,j\le n+1} \in M_{n+1}(\mathbb{Z})$ where a_{ij} is an integer satisfying

$$\Phi_{[\mathbf{r},\mathbf{s};1,i]}(z_\ell)_p^{\left(\frac{K_1/k}{(\omega_{1,j})}\right)} = \zeta_p^{a_{ij}} \Phi_{[\mathbf{r},\mathbf{s};1,i]}(z_\ell)_p$$

for all odd primes p. Note that $A_\ell(\mathbf{r}, \mathbf{s})$ does not depend on p by lemma 6.2.

THEOREM 6.3. *Let ℓ and p be odd primes, $n = \frac{\ell-1}{2}$ and $\mu \in \mathbb{N}$. And, let $\mathbf{r}$, $\mathbf{s}$, z_ℓ and $A_\ell(\mathbf{r}, \mathbf{s})$ be as above. Assume that z_ℓ is neither a zero nor a pole of $\prod_{i=1}^{n+1} \Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z)_p$. If $p \nmid \ell h_\ell^+ n \cdot \det\big(A_\ell(\mathbf{r}, \mathbf{s})\big)$, then we have*

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,1]}(z_\ell)_p^{p^\alpha}, \Phi_{[\mathbf{r},\mathbf{s};\mu,2]}(z_\ell)_p^{p^\alpha}, \dots, \Phi_{[\mathbf{r},\mathbf{s};\mu,n+1]}(z_\ell)_p^{p^\alpha}\big) \tag{6.2}$$

for $0 \le \alpha \le \mu - 1$. *Moreover, if* $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = n-1$ *then we get*

$$k_{2\mu-\alpha} = k_\mu\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,1]}(z_\ell)_p^{p^\alpha}, \Phi_{[\mathbf{r},\mathbf{s};\mu,2]}(z_\ell)_p^{p^\alpha}, \dots, \Phi_{[\mathbf{r},\mathbf{s};\mu,n+1]}(z_\ell)_p^{p^\alpha}\big) \tag{6.3}$$

for $0 \le \alpha \le \mu - 1$.

Proof. Let $\mathbf{x}_{\mu,i} = \frac{1}{p^\mu} r_i$ and $\mathbf{y}_{\mu,i} = \frac{1}{p^\mu} s_i$ for each μ and i. Then $\mathbf{x}_{\mu,i} = \frac{1}{p^{\mu-1}}\mathbf{x}_{1,i}$ and $\mathbf{y}_{\mu,i} = \frac{1}{p^{\mu-1}}\mathbf{y}_{1,i}$. By Lemma 6.1, $\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha} \in K_{2\mu-1-\alpha}$. From the formula (6.1) we obtain for $1 \le i, j \le n+1$

$$\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha}\big)^{\left(\frac{K_{2\mu-1-\alpha}/k}{(\omega_{2\mu-1-\alpha,j})}\right)} = e(-p^{2\mu-1}\cdot {}^t\mathbf{x}_{\mu,i}\mathbf{y}_{\mu,i})e\Big(\frac{{}^t\mathbf{x}_{\mu,i}b_{2\mu-1,j} - {}^t a_{2\mu-1,j}\mathbf{y}_{\mu,i}}{2}\Big)\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha},$$

where $a_{2\mu-1,j}, b_{2\mu-1,j} \in 2p^{\mu-1}\mathbb{Z}^n$ such that

$$\begin{aligned}\begin{pmatrix} a_{2\mu-1,j} \\ b_{2\mu-1,j}\end{pmatrix} &= 2p^{2\mu-1}\cdot {}^t h\big(\varphi^+(\zeta^j)\big)\begin{pmatrix}\mathbf{x}_{\mu,i}\\ \mathbf{y}_{\mu,i}\end{pmatrix} \\ &= 2p^{\mu}\cdot {}^t h\big(\varphi^+(\zeta^j)\big)\begin{pmatrix}\mathbf{x}_{1,i}\\ \mathbf{y}_{1,i}\end{pmatrix} \\ &= p^{\mu-1}\begin{pmatrix} a_{1,j} \\ b_{1,j}\end{pmatrix}.\end{aligned}$$

Hence we ensure

$$\begin{aligned}\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha}\big)^{\left(\frac{K_{2\mu-1-\alpha}/k}{(\omega_{2\mu-1-\alpha,j})}\right)} &= e(-p\cdot {}^t\mathbf{x}_{1,i}\mathbf{y}_{1,i})e\Big(\frac{{}^t\mathbf{x}_{1,i}b_{1,j} - {}^t a_{1,j}\mathbf{y}_{1,i}}{2}\Big)\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha} \\ &= \zeta_p^{a_{ij}}\Phi_{[\mathbf{r},\mathbf{s};\mu,i]}(z_\ell)_p^{p^\alpha},\end{aligned} \tag{6.4}$$

where a_{ij} is the $(i,j)^{\text{th}}$ entry of $A_\ell(\mathbf{r},\mathbf{s})$. Now, we observe that for $1 \le i \le n+1$ there exists $\gamma_i \in k_{2\mu-1-\alpha}\big(\Phi_{[\mathbf{r},\mathbf{s};\mu,1]}(z_\ell)_p^{p^\alpha}, \Phi_{[\mathbf{r},\mathbf{s};\mu,2]}(z_\ell)_p^{p^\alpha}, \dots, \Phi_{[\mathbf{r},\mathbf{s};\mu,n+1]}(z_\ell)_p^{p^\alpha}\big)$ with

$$\gamma_i^{\left(\frac{K_{2\mu-1-\alpha}/k}{(\omega_{2\mu-1-\alpha,j})}\right)} = \begin{cases} \zeta_p\gamma_i & \text{if } \ j = i \\ \gamma_i & \text{if } j \ne i\end{cases}$$

because $p \nmid \det(A_\ell(\mathbf{r},\mathbf{s}))$. Since $\big|\mathrm{Gal}(K_{2\mu-1-\alpha}/k_{2\mu-1-\alpha})\big| \le p^{n+1}$ by (5.1), we derive

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\big(\gamma_1, \gamma_2, \dots, \gamma_{n+1}\big).$$

Therefore (6.2) is proved.

If $\dim_{\mathbb{Z}/p\mathbb{Z}}(H_1/S_2) = n-1$, then from the proof of Corollary 5.6 we get

$$|\mathrm{Gal}(k_{2\mu-\alpha}/k_{2\mu-1-\alpha})| = p^{n+1}.$$

Since $\big|\mathrm{Gal}(K_{2\mu-1-\alpha}/k_{2\mu-1-\alpha})\big| = p^{n+1}$ and $K_{2\mu-1-\alpha} \subset k_{2\mu-\alpha}$, we conclude $K_{2\mu-1-\alpha} = k_{2\mu-\alpha}$. Hence (6.3) is proved by (6.2). □

Although we omit in the above theorem the case where p divides $\det(A_\ell(\mathbf{r},\mathbf{s}))$, by utilizing Theorem 5.5 we might find suitable generators of K_μ over k_μ for each $\mu \in \mathbb{N}$.

Let $\mathbf{r_0} = (r_i)_{1\le i\le n+1}$ and $\mathbf{s_0} = (s_i)_{1\le i\le n+1}$ where $r_i = {}^t(1,0,\dots,0) \in \mathbb{Z}^n$ and $s_i = {}^t\big((s_i)_j\big)_{1\le j\le n} \in \mathbb{Z}^n$ for $1 \le i \le n+1$ with

$$(s_i)_j = \begin{cases} 1 & \text{if } \ j < i \\ 0 & \text{otherwise.} \end{cases}$$

Here we observe that $\Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,i]}(z)_p$ is not identically zero for all μ and i by Proposition 3.3.

Corollary 6.4. *Let ℓ and p be odd primes and z_ℓ be as above. Put $n = \frac{\ell-1}{2}$ and $\mu \in \mathbb{N}$. Further, we assume that z_ℓ is neither a zero nor a pole of $\displaystyle\prod_{i=1}^{n+1} \Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,i]}(z)_p$.*

(i) *Let $\ell = 7$. If $p \ne 3, 7$, then we have*

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\big(\Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,1]}(z_7)_p^{p^\alpha}, \Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,2]}(z_7)_p^{p^\alpha}, \dots, \Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,4]}(z_7)_p^{p^\alpha}\big) \tag{6.5}$$

for $0 \le \alpha \le \mu - 1$.

(ii) *Let $\ell = 11$. If $p \ne 3, 5, 11$, then we have*

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\big(\Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,1]}(z_{11})_p^{p^\alpha}, \Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,2]}(z_{11})_p^{p^\alpha}, \dots, \Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,6]}(z_{11})_p^{p^\alpha}\big) \tag{6.6}$$

for $0 \le \alpha \le \mu - 1$. And, if $p = 3$ then we get

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\big(\Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,1]}(z_{11})_3^{3^\alpha}, \Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,2]}(z_{11})_3^{3^\alpha}, \dots, \Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,5]}(z_{11})_3^{3^\alpha}\big). \tag{6.7}$$

(iii) *Let $\ell = 13$. If $p \ne 3, 5, 13$, then we have*

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\big(\Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,1]}(z_{13})_p^{p^\alpha}, \Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,2]}(z_{13})_p^{p^\alpha}, \dots, \Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,7]}(z_{13})_p^{p^\alpha}\big) \tag{6.8}$$

for $0 \le \alpha \le \mu - 1$. And, if $p = 5$ then we get

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\big(\Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,1]}(z_{13})_5^{5^\alpha}, \Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,2]}(z_{13})_5^{5^\alpha}, \dots, \Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,6]}(z_{13})_5^{5^\alpha}\big). \tag{6.9}$$

(iv) *Let $\ell = 5$. Then we have*

$$K_{2\mu-1-\alpha} = k_{2\mu-1-\alpha}\big(\zeta_{p^{2\mu-\alpha}}, \Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,1]}(z_5)_p^{p^\alpha}, \Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,3]}(z_5)_p^{p^\alpha}\big) \tag{6.10}$$

for $0 \le \alpha \le \mu - 1$.

PROOF. Let the matrix $M_\ell(p)$ be as in Lemma 5.4. Note that $h_\ell^+ = 1$ for $\ell \leq 67$ ([11, p.352]).

(i) Using the formula (6.1) we can find $\Phi_{[\mathbf{r_0},\mathbf{s_0};1,i]}(z_7)_p^{\left(\frac{K_1/k}{(\omega_{1,j})}\right)}$ for each $1 \leq i,j \leq 4$ as follows:

$$\begin{array}{c} \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,1]}(z_7)_p \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,2]}(z_7)_p \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,3]}(z_7)_p \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,4]}(z_7)_p \end{array} \begin{array}{c} \begin{array}{cccc} \left(\frac{K_1/k}{(\omega_{1,1})}\right) & \left(\frac{K_1/k}{(\omega_{1,2})}\right) & \left(\frac{K_1/k}{(\omega_{1,3})}\right) & \left(\frac{K_1/k}{(\omega_{1,4})}\right) \end{array} \\ \begin{pmatrix} -1 & -1 & -1 & 1 \\ -2 & -4 & -2 & 0 \\ 0 & -10 & -4 & 2 \\ -3 & -13 & -11 & 9 \end{pmatrix} \end{array} = A_7(\mathbf{r_0},\mathbf{s_0}).$$

Since $\det(A_7(\mathbf{r_0},\mathbf{s_0})) = 2^6$ is prime to p, (6.5) is true by Theorem 6.3.

(ii) First, suppose that $p \neq 3, 5, 11$. In a similar way as in (i) we obtain

$$A_{11}(\mathbf{r_0},\mathbf{s_0}) = \begin{pmatrix} -1 & -1 & -1 & -1 & -1 & 1 \\ -2 & -4 & -2 & -4 & -2 & 0 \\ -4 & -6 & -4 & -10 & 0 & -2 \\ -7 & -3 & -11 & -21 & -3 & 1 \\ -7 & -5 & -25 & -29 & -1 & -1 \\ -10 & -2 & -48 & -34 & -6 & 4 \end{pmatrix}.$$

Since $\det(A_{11}(\mathbf{r_0},\mathbf{s_0})) = 2^7 \cdot 3 \cdot 5^2$ is prime to p, we get (6.6) by Theorem 6.3. If $p = 3$, then the rank of $M_{11}(3)$ is equal to 5. Since $p \nmid 11 \cdot 5$, by Theorem 5.5 we obtain $\mathrm{Gal}(K_\mu/k_\mu) \cong (\mathbb{Z}/3\mathbb{Z})^5$ for all $\mu \in \mathbb{N}$. And we observe that the determinant of the matrix

$$\begin{array}{c} \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,1]}(z_{11})_3 \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,2]}(z_{11})_3 \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,3]}(z_{11})_3 \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,4]}(z_{11})_3 \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,5]}(z_{11})_3 \end{array} \begin{array}{c} \begin{array}{ccccc} \left(\frac{K_1/k}{(\omega_{1,2})}\right) & \left(\frac{K_1/k}{(\omega_{1,3})}\right) & \left(\frac{K_1/k}{(\omega_{1,4})}\right) & \left(\frac{K_1/k}{(\omega_{1,5})}\right) & \left(\frac{K_1/k}{(\omega_{1,6})}\right) \end{array} \\ \begin{pmatrix} -1 & -1 & -1 & -1 & 1 \\ -4 & -2 & -4 & -2 & 0 \\ -6 & -4 & -10 & 0 & -2 \\ -3 & -11 & -21 & -3 & 1 \\ -5 & -25 & -29 & -1 & -1 \end{pmatrix} \end{array}$$

is equal to $2^5 \cdot 5 \cdot 11$ which is prime to 3. Using the formulas (6.4) we can conclude (6.7).

(iii) First, suppose that $p \neq 3, 5, 13$. Then we derive

$$A_{13}(\mathbf{r_0}, \mathbf{s_0}) = \begin{pmatrix} -1 & -1 & -1 & -1 & -1 & -1 & 1 \\ -2 & -4 & -2 & -4 & -2 & -4 & 2 \\ 0 & -10 & -4 & -6 & -4 & -10 & 8 \\ 5 & -19 & -7 & -11 & -11 & -13 & 11 \\ 7 & -35 & -13 & -13 & -19 & -15 & 13 \\ 2 & -60 & -18 & -8 & -32 & -22 & 20 \\ -10 & -84 & -28 & 2 & -54 & -22 & 20 \end{pmatrix}.$$

Since $\det(A_{13}(\mathbf{r_0}, \mathbf{s_0})) = -2^{12} \cdot 5^2$ is prime to p, we have (6.8) again by Theorem 6.3. If $p = 5$, then the rank of $M_{13}(5)$ is equal to 6. Since $p \nmid 13 \cdot 6$, it follow from Theorem 5.5 that $\mathrm{Gal}(K_\mu/k_\mu) \cong (\mathbb{Z}/5\mathbb{Z})^6$ for all $\mu \in \mathbb{N}$. Observe that the determinant of the matrix

$$\begin{array}{c} \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,1]}(z_{13})_5 \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,2]}(z_{13})_5 \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,3]}(z_{13})_5 \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,4]}(z_{13})_5 \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,5]}(z_{13})_5 \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,6]}(z_{13})_5 \end{array} \begin{array}{c} \begin{pmatrix} \frac{K_1/k}{(\omega_{1,2})} \end{pmatrix} \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{pmatrix} \frac{K_1/k}{(\omega_{1,3})} \end{pmatrix} \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{pmatrix} \frac{K_1/k}{(\omega_{1,4})} \end{pmatrix} \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{pmatrix} \frac{K_1/k}{(\omega_{1,5})} \end{pmatrix} \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{pmatrix} \frac{K_1/k}{(\omega_{1,6})} \end{pmatrix} \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{pmatrix} \frac{K_1/k}{(\omega_{1,7})} \end{pmatrix} \\ \\ \\ \\ \\ \\ \end{array}$$
$$\begin{pmatrix} -1 & -1 & -1 & -1 & -1 & 1 \\ -4 & -2 & -4 & -2 & -4 & 2 \\ -10 & -4 & -6 & -4 & -10 & 8 \\ -19 & -7 & -11 & -11 & -13 & 11 \\ -35 & -13 & -13 & -19 & -15 & 13 \\ -60 & -18 & -8 & -32 & -22 & 20 \end{pmatrix}$$

is equal to $-2^7 \cdot 31$ which is prime to 5. Using the formulas (6.4) we can ensure (6.9).

(iv) In this case $\det(A_5(\mathbf{r_0}, \mathbf{s_0})) = 0$ so that we should find another generators of $K_{2\mu-1-\alpha}$ over $k_{2\mu-1-\alpha}$. By [4, p.316], $H_{2\mu-1-\alpha}/S_{2\mu-\alpha}$ is generated by real units of k for any odd prime p. Using the idea of the proof of Theorem 5.5, one can show that $(\varphi^*(S_{2\mu-1-\alpha}) \cap H_{2\mu-1-\alpha})/S_{2\mu-\alpha} = \{0\}$, and so $\Phi_{[\mathbf{r_0},\mathbf{s_0};\mu,i]}(z_5)_p^{p^\alpha} \in K_{2\mu-1-\alpha}$ for $1 \leq i \leq 3$. Note that $\zeta_{p^{2\mu-\alpha}} \in \mathfrak{A}_0\big(\Gamma(2p^{2\mu-\alpha}), \mathbb{Q}(\zeta_{2p^{2\mu-\alpha}})\big)$ is $R_{2p^{2\mu-\alpha}}$-invariant, hence $\zeta_{p^{2\mu-\alpha}} \in K_{2\mu-1-\alpha}$ by Proposition 4.2. Since $N_{k/\mathbb{Q}}(\omega_{2\mu-1-\alpha,j}) \equiv 1 - 2p^{2\mu-1-\alpha} \pmod{2p^{2\mu-\alpha}}$ for $1 \leq j \leq 3$, we get

$$\zeta_{p^{2\mu-\alpha}}^{\left(\frac{K_{2\mu-1-\alpha}/k}{(\omega_{2\mu-1-\alpha,j})}\right)} = \zeta_p^{-2}\zeta_{p^{2\mu-\alpha}} \quad \text{for } 1 \leq j \leq 3. \tag{6.11}$$

Now, observe that the determinant of the matrix

$$\begin{array}{c} \\ \zeta_{p^2} \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,1]}(z_5)_p \\ \Phi_{[\mathbf{r_0},\mathbf{s_0};1,3]}(z_5)_p \end{array} \begin{array}{c} \begin{pmatrix} \frac{K_1/k}{(\omega_{1,1})} \end{pmatrix} \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{pmatrix} \frac{K_1/k}{(\omega_{1,2})} \end{pmatrix} \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{pmatrix} \frac{K_1/k}{(\omega_{1,3})} \end{pmatrix} \\ \\ \\ \\ \end{array}$$
$$\begin{pmatrix} -2 & -2 & -2 \\ -1 & -1 & 1 \\ -4 & -6 & 4 \end{pmatrix}$$

is equal to -2^3 which is prime to p. Therefore, we obtain (6.10) by (6.4) and (6.11).

□

REMARK 6.5. (i) Especially when $\mu = 1$, Corollary 6.4 (iv) is reduced to Komatsu's work ([4, Proposition 1]) with a little different ingredients.

(ii) The following table provides prime factors of $\det(A_\ell(\mathbf{r_0}, \mathbf{s_0}))$ for $\ell \leq 89$.

ℓ	prime factors of $\det(A_\ell(\mathbf{r_0}, \mathbf{s_0}))$
3	2
5	0
7	2
11	2, 3, 5
13	2, 5
17	2, 7, 17, 43
19	2, 3, 36137
23	2, 3, 11, 13, 29, 89, 241
29	2, 3, 5, 13, 113, 58057291
31	2, 3, 31, 109621, 1216387
37	2, 5, 13, 37, 53, 109, 10138325056259
41	2, 5, 11, 17, 41, 439, 1667, 166013, 203381
43	2, 3, 19, 43, 211, 281345721890371109
47	2, 5, 83, 139, 5323, 178481, 6167669171116393
53	2, 3, 5, 139, 157, 1613, 4889, 1579367, 28153859844430949
59	2, 3, 59, 233, 3033169, 189946818040963445273025207051 7
61	2, 5, 11, 13, 41, 1321, 1861, 1142941857599125232990619467569
67	2, 3, 67, 683, 12739, 20857, 513881, 1858283767, 986862333655510350967
71	2, 5, 7, 31, 79, 127, 1129, 79241, 122921, 68755411, 1190061671, 3087543529906501
73	2, 7, 73, 79, 89, 16747, 134353, 5754557119657, 1150806776867233, 1190899
79	2, 5, 7, 13, 29, 53, 1427, 3847, 8191, 121369, 377911, 1842497, 51176893, 357204083, 32170088152177
83	2, 3, 13, 17387, 279405653, 430592619820725846267877053013 51, 8831418697, 758583423553
89	2, 17, 23, 89, 113, 313629821584641896139082338756559409, 4504769, 118401449, 22482210593

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976.

[2] J. Igusa, *On the graded ring of theta-constants (II)*, Amer. J. Math. 88 (1966) 221-236.

[3] H. Klingen, *Introductory Lectures on Siegel Modular Forms*, Cambridge Studies in Advanced Mathematics, 20, Cambridge University Press, Cambridge, 1990.

[4] K. Komatsu, *Construction of a normal basis by special values of Siegel modular functions*, Proc. Amer. Math. Soc. 128 (2000), no. 2, 315-323.

[5] S. Lang, *Elliptic Functions*, 2nd ed., Spinger-Verlag, New York, 1987.

[6] J. Liang, *On the integral basis of the maximal real subfield of a cyclotomic field*, J. reine angew. Math. 286/287 (1976), 223-226.

[7] G. Shimura, *Theta functions with complex multiplication*, Duke Math. J. 43 (1976), no. 4, 673-696.

[8] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, Princeton, NJ, 1998.

[9] G. Shimura, *On canonical models of arithmetic quotients of bounded symmetric domains*, Ann. of Math. (2) 91 (1970) 144-222.

[10] G. Shimura, *On canonical models of arithmetic quotients of bounded symmetric domains II*, Ann. of Math. (2) 92 (1970), 528-549.

[11] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.

Ja Kyung Koo
Department of Mathematical Sciences
KAIST
Daejeon 305-701
Republic of Korea

E-mail address: jkkoo@math.kaist.ac.kr

Dong Sung Yoon
Department of Mathematical Sciences
KAIST
Daejeon 305-701
Republic of Korea

E-mail address: yds1850@kaist.ac.kr